Big Sandy Rural Electric
Cooperative Corporation

504 11th Street
Paintsville, Kentucky 41240-1422
(606) 789-4095 • Fax (606) 789-5454
Toll Free (888) 789-RECC (7322)

ORIGINAL

June 10, 2016

Executive Director
Public Service Commission
211 Sower Blvd.
Frankfort, KY 40602

RE: Public Service Commission Case No. 2012-00428

Dear Executive Director:

Please find enclosed the original and 3 copies of Big Sandy Rural Electric Cooperative Corporation's response to the April 13, 2016 Order pertaining to Case No. 2012-00428. Billy Frasure will be the witness responsible for responding to the questions related to the information provided.

If you should need any additional information, please do not hesitate to contact me.

Thank you,

David Estepp

David Estepp
President & General Manager

CERTIFICATE

STATE OF KENTUCKY)
COUNTY OF JOHNSON)

Billy O. Frasure, CPA, being duly sworn, states that he has supervised the preparation of the response of Big Sandy RECC to the Public Service Commission Staff's Request for information in the above-referenced Case No. 2012-00428 dated April 13, 2016 and that the matters and things set forth therein are true and accurate to the best of his knowledge, information and belief, formed after reasonable inquiry.

Billy Frasure

Billy O. Frasure, CPA

Subscribed and sworn before me on this 10th day of June, 2016

Judy L. McClure

Notary Public

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION
PSC CASE NO. 2012-00428
RESPONSE TO COMMISSION'S ORDER

REQUEST 4

Within 60 days of the date of this Order, the Joint Utilities should file with the Commission their internal procedures governing customer privacy and customer education.

RESPONSE 4

Please see Exhibit 1 and Exhibit 2 for Big Sandy's internal procedures governing customer privacy. Customer education is achieved using various methods. Big Sandy utilizes various resources such as its website, Kentucky Living magazine and social media (Facebook) to provide information to its customers.

Witness: Billy Frasure

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION
PSC CASE NO. 2012-00428
RESPONSE TO COMMISSION'S ORDER

REQUEST 5

Within 60 days of the date of this Order, the Joint Utilities shall certify to the Commission that they have developed internal cybersecurity procedures.

RESPONSE 5

Please refer to Exhibit 3.

Witness: Billy Frasure

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION
PSC CASE NO. 2012-00428
RESPONSE TO COMMISSION'S ORDER

REQUEST 10

Within 60 days of the date of this Order, the jurisdictional electric utilities shall file with the Commission their internal procedures regarding Smart Grid Investments.

RESPONSE 10

Smart Grid Investments

This document addresses aspects of smart grid investments.

System Description

Big Sandy RECC is a rural electric cooperative headquartered in Paintsville in Johnson County, Kentucky. Big Sandy's electric distribution system consists of over 1,000 miles of line which operate at 7,620/13,200 volts.

At the end of 2015 the number of consumers served was 12,990. The consumer base is over 92% residential and less than 8% commercial and industrial.

Big Sandy RECC began installation of an AMI system in 2005 and completed the installation in 2008. The AMI system is now known as the Aclara TWACS system.

In response to a need for alternative payment methods for our consumers, Big Sandy RECC began investigating prepay metering. Prepay Metering is a technology which is available through the Aclara TWACS system. A pilot tariff for prepay metering was approved by the PSC in March, 2013 Case No. 2012-00425 and a permanent tariff was approved in April, 2016 Case No. 2015-00337. As of June 2016 there are 224 active prepay metering accounts.

Big Sandy RECC has implemented a Meter Data Management System (MDMS) that enables members to view their electric usage via a member portal. The data from the AMI system makes the MDMS system work in a timely manner. By updating the consumer usage data on an hourly basis, instead of once a month, the member has more timely information about their usage.

Big Sandy RECC has an Outage Management System (OMS) for tracking outage information. The AMI system works with the OMS allowing the dispatcher to ping a meter to determine if it is on or off.

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION
PSC CASE NO. 2012-00428
RESPONSE TO COMMISSION'S ORDER

Planning Goals

Investments in smart grid technology must be consistent with the cooperative's goal of providing reliable electric service at a reasonable price.

Big Sandy RECC will continue to evaluate new technologies as they become available. A part of that consideration will be to what degree the new technology will work with other smart grid technologies that may be in place at the time of evaluation.

As of this time, Big Sandy RECC has no immediate plans for new investments in smart grid technologies.

How Smart Grid Investments Will Be Considered

Investment in new smart grid technology will be made when it makes prudent economic sense for Big Sandy RECC's members

Any new AMI system would be included in Big Sandy's Construction Work Plan and would be submitted to the Commission and Rural Utilities Service (RUS) for review and approval.

Witness: Billy Frasure

EXHIBIT 17
PAGE 1 OF 6

Big Sandy Rural Electric Cooperative Corporation

Board Policy No. 300-099
Identity Theft Prevention Program

NOW, THEREFORE BE IT RESOLVED, that this adoption was properly authorized by the Board of Directors during a monthly Board of Directors meeting held on October 22, 2008.

I, Joe W. Harris, Jr. Secretary/Treasurer of the Big Sandy Rural Electric Cooperative Corporation hereby certify that the foregoing is a full, true, and correct copy of the duly passed by the Board of Directors of Big Sandy Rural Electric Cooperative at a meeting duly called and held in compliance with the By-Laws of the Cooperative on the 22nd day of October, 2008, at which meeting a quorum was present, and that the Policy Adoption as set out above appears in the minutes of that meeting in the Minutes Book of the Cooperative dated this 22nd day of October, 2008.

SOURCE: ADOPTED October 22, 2008

Joe Harris

JOE W. HARRIS, JR., SECRETARY/TREASURER

EXHIBIT 1
PAGE 2 OF 6

ORIGINAL

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATIVE
POLICY NO. 300-099
SECTION C

SUBJECT: **Big Sandy RECC** has developed an **Identity Theft Prevention Program.**

OBJECTIVE: Designed to detect, prevent and mitigate theft in connection with the opening or maintaining of any covered account. The program is consistent with the utility's mission to provide safe and reliable electricity at the lowest possible price, while being an active and supportive part of the communities we serve.

Privacy Committee

On November 1, 2008, the Privacy Committee was formed under the leadership of representation from key areas included:

Name	Department	Responsibilities
Jeff Prater	Senior Management	**Operations Management Field Employees**
Sandra Shepherd	Accounting	**Billing & Collections Expert in the Flow of Funds**
Adam Ferguson	IT	**Data and Network Security Expert in Network Admin.**
Trish Baldwin	Payroll & HR	**Employee-Employer related business. Personnel Information. Identify Theft Training**
Angie Stewart	Customer Resources	**Day to day processes in opening new accounts and monitoring activity of existing accounts**

EXHIBIT 1
PAGE 3 OF 6

Judy McClure	HR & Administration	**Privacy Officer** **Will coordinate activities of the committee, develop and evaluate program** **Reports to Senior Mgt & Board of Directors**

Our Privacy Committee will attend scheduled meetings every six months, and minutes will be taken. An annual report will be presented to the Board for review. A Policy handbook (manual) will be used in establishing guidelines and regulations and will be administered to train all necessary employees.

I. Purpose:

The goal of this policy is to prevent identity theft. Big Sandy RECC recognizes the responsibility to safeguard personal customer information within the workplace. The purpose of this policy is to create an Identity Theft Prevention Program utilizing guides set forth in the FACT Act (2003).

II. Scope:

This policy applies to management and all personnel of Big Sandy RECC. The following represents a policy for the development of the Identity Theft Prevention program. Company may already have policies written and developed, which can be incorporated into the program. This does not replace, but rather supplements, any standing policies.

III. Responsibility:

Big Sandy RECC must protect customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by November 1, 2008.

EXHIBIT 1
PAGE 4 OF 6

IV. Definitions:

IT – Information Technology

Identity Theft – Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit card accounts, establishing lines of credit, or gaining access to victim's accounts with the intent of depleting the balances.

Company – For the purposes of this policy, Big Sandy RECC is referred to as Company.

Red Flag – A pattern, particular specific activity that indicates the possible risk of identity theft.

V. Procedure:

A. Implementing the Program

1. Form an Identity Theft Prevention Protection Committee. Establish an Identity Theft Prevention Committee to create, drive and monitor the program. Select members from Senior Management, Accounting, IT, Human Resources, Administration and Customer Service.

2. Assign Responsibilities to Committee Members.

3. Appoint a Privacy Officer

Privacy officer functions as the head of committee. He/she reports to a member of Senior Management, i.e.: General Manager regarding the outcomes and needs of the identity theft prevention program.

EXHIBIT 1
PAGE 5 OF 6

B. Assess Company's Need for New/Updated Policies and Procedure

The following represent the core of the procedures for the Identity Theft Prevention Program. Please modify to meet the needs and standards of your utility. Add related policies such as "Use of Passwords," as they are already established.

IV. Providing Designated Employees with Identity Theft Prevention Training

1. Designated employees will be trained on a need to know basis according to job responsibilities.

2. Initial training is provided on 3 levels:

   Committee members participated in a 12 hour professional association Identity Theft Prevention Program workshop covering principles of needs assessment, program design, development, implementation and evaluation. Strategies for revision and reporting were included. Committee members unable to attend will receive one on one training by a workshop attendee.

   Supervisors – Initial two hour program addresses supervisory role in preventing identity theft.

   Employee – Initial two hour program addresses the safeguarding of secured information.

3. Annual Updates will be provided for all designated employees. Sessions to be a minimum of 30 minutes will include, but not limited to:

   Patterns of incidents, changes in informational technology, changes in methods of Identity theft, results of evaluations, employee's input on strategies for enhancing Identity Theft Prevention Program.

4. Documentation of Training

EXHIBIT 1
PAGE 6 OF 6

Needs Assessment

On November 1, 2008, Big Sandy RECC conducted a needs assessment of the flow of secured information during the processes of opening a new account as well as monitoring transactions on existing accounts. A review of red flags in the industry and the examples outlined in the FACT Act legislation served as the basis for comparing present policies and procedures against those needed to detect, prevent and mitigate identity theft. The following strengths and areas for improvement were identified:

Opening Accounts:

Strengths: Photos IDs, such as State ID card, Driver's License and obtaining a social security card. Using Online Utility to verify. Computer monitors hid away from plain view.

Areas for Improvement: Opening accounts in a private office so no one can over hear conversation. Keeping service order out of view and removing social security off of service orders. Shred all notes!

Monitoring Transactions in Existing Accounts:

Strengths: Online bill payments – When someone calls in we ask questions long the lines of social security number, telephone number, address and password questions that they have setup. If someone calls for help on setting an online account up, we verify again with the social security number and address questions. If someone tries to use it to setup a new account, we know they already have an existing account because we monitor social security numbers.

Areas for Improvement: Monitoring credit card use with credit card logs. Locking computer down when CSR leaves for break!! New user log in and out when filling in for the CSRs, so not just anyone can look at the information on the screen by walking around to it. When mail is being dropped off, it is handed to an employee and not just set down on a desk when someone is not at that desk!!!

EXHIBIT 2

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION

SECTION C – ADMINISTRATION

POLICY # 300-182

SUBJECT: **Social Media Policy**

PURPOSE: **To establish a policy that addresses the appropriate use of Cooperative equipment and software, for communication thru Social Media Networks.**

POLICY: **Big Sandy RECC's Social Media Policy states the guidelines for all employees accessing the internet, Facebook, Twitter, email and all avenues of social media networks. The use of Facebook and Twitter are authorized by Big Sandy RECC, with certain purposes. The use of the above Social Media Networks shall be restricted to information coming from Big Sandy RECC. The Manager of Member Services and Public Relations has responsibility for any information that may be posted.**

PROVISIONS/RESTRICTIONS

The possibility of breaches to the security of confidential Company information is the hazard we hope to avoid. Internet use brings the possibility of contamination to our systems via viruses or spyware. Spyware allows unauthorized people, outside the Company, potential access to Company passwords and other confidential information.

1. The Cooperative reserves the right to block access to individual sites as deemed appropriate by Management.
2. The Cooperative reserves the right to limit access by individual employees to the Internet and other systems as deemed appropriate by Management.
3. Employees recognize that their Internet activity can be tracked by the Co-Op and sites visited can be viewed by system administrators at any time.
4. Employees realize that emails sent from, received by or forwarded using Co-Op equipment is tracked, stored and subject to review by system administrators. These communications cannot be classified as private and confidential when sent using Cooperative equipment.
5. The strategy for using Social Media is to enhance Big Sandy RECC's ability to quickly and easily post short communications to the BSRECC website or to others that follow our informational posts. The use of Facebook and Twitter shall be restricted to information coming from BSRECC. The strategies for using either of these Social Media Networks shall be reviewed and updated as necessary.
6. Employees must follow all Co-Op policies, procedures and guidelines when using Internet, voice mail, email and Social Media for company purposes. Employees must realize that they are subject to legal actions, for liable, slander, defamation, plagiarism and copyright infringement. Employees are not entitled to legal defense by the Co-Op in these situations.
   a. Employees further realize that their actions also expose the Co-Op to similar legal actions.

Big Sandy RECC respects the right of employees to use these Social Media Networks during their personal time and with their personal equipment. However, use of these communication tools, on company time or equipment will be under subjection of the President/General Manager's approval. Employees must avoid posting information that could harm Big Sandy RECC. Breaching of this

EXHIBIT 2
PAGE 2 OF 2

policy by any Big Sandy RECC employee will result to disciplinary action determined by the President/General Manager

RESPONSIBILITY: President/General Manager shall be responsible for the administration of this policy.

Adopted: JULY 27, 2011

David Estepp

President/General Manager

Secretary of the Board

EXHIBIT 3
PAGE 1 OF 21

BIG SANDY RURAL ELECTRIC COOPERATIVE CORPORATION

POLICY STATEMENT NO. 300-191

SECTION C

POLICY: **CYBER SECURITY POLICY**

PURPOSE: This policy is to ensure compliance with the implementation for outlining of standards and procedures used to protect Big Sandy RECC's informational assets whether stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on electronic or optical media or spoken from all threats, whether internal or external, deliberate or accidental.

PROCEDURE: A Cyber Security Handbook "Attachment A" has been developed for the compliance and adherence to the Cyber Security Policy. The General Manager has approved the Cyber Security Handbook. The Cyber Security policy for Big Sandy RECC is to ensure that:

A. Information will be protected against accidental unauthorized access.

B. Confidentiality must ensure the protection of valuable and/or sensitive information from unauthorized disclosure or intelligible interruption.

C. Integrity of information will maintain the accuracy and completeness of information by protecting against unauthorized modification.

D. Regulatory and legislative requirements will be met.

E. Business Continuity plans will be produced, maintained, and tested to ensure that information and vital services are available to users when they need them.

F. Information Security Training will be available and mandatory to all employees.

ALL BREACHES OF INFORMATION SECURITY, ACTUAL OR SUSPECTED WILL BE REPORTED AND INVESTIGATED BY THE BIG SANDY RECC IT DEPARTMENT.

RESPONSIBILITY: **The Big Sandy IT Department has direct responsibility for maintaining this Handbook "Attachment A" and providing guidance and advice on its implementation in adherence to this adopted Cyber Security Policy. The Handbook will be revised to reflect changes in the security process and procedures, without the necessity of adopting a new policy (No. 300-191), Section C. It is the responsibility of EACH EMPLOYEE of Big Sandy RECC to adhere to this policy.**

ADOPTED: 9-25-2014

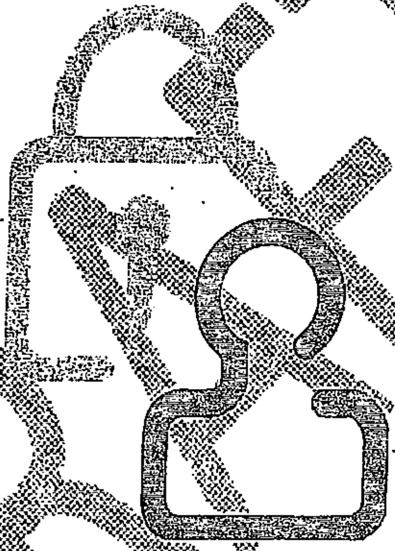
Secretary

ATTACHMENT "A"

EXHIBIT 3
PAGE 2 OF 21

Cyber Security Handbook

Big Sandy RECC



Standards, Procedures and Guidelines

Version 1.0

Adam Ferguson

EXHIBIT 3
PAGE 3 OF 21

CONTENTS

EXHIBIT 3
PAGE 4 OF 21

CORPORATE INFORMATION SECURITY

Security Statement

The purpose of this handbook is to outline standards and procedures used to protect the company's information assets whether stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on electronic or optical media, or spoken from all threats, whether internal or external, deliberate or accidental.

The General Manager has approved the Cyber Security Handbook. It is the policy of Big Sandy RECC to ensure that:

- Information will be protected against accidental unauthorized access.
- Confidentiality must ensure the protection of valuable and/or sensitive information from unauthorized disclosure or intelligible interruption.
- Integrity of information will maintain the accuracy and completeness of information by protecting against unauthorized modification.
- Regulatory and legislative requirements will be met.
- Business Continuity plans will be produced, maintained, and tested to ensure that information and vital services are available to users when they need them.
- Information Security training will be available to all employees.

All breaches of information security, actual or suspected, will be reported and investigated by the Big Sandy RECC IT Department.

The Big Sandy RECC IT Department has direct responsibility for maintaining this handbook and providing guidance and advice on its implementation.

It is the responsibility of EACH employee to adhere to this Cyber Security Handbook.

EXHIBIT 3

INTRODUCTION

About this Handbook

This handbook outlines information security standards, procedures and guidelines that are utilized by Big Sandy RECC employees – they form the foundation for the Big Sandy RECC Cyber Security Program.

Compliance with the contents is mandatory.

The manual is the responsibility of the Big Sandy RECC IT Security Department, which will ensure that the statements within it reflect changing business and technological needs. Further detail on the responsibilities and the process of change control are given later.

Using the Standards

The manual is intended as a reference document to ensure that our practices and procedures are implemented in a consistent fashion across the company.

Change Control

The manual is intended to be a "living" document and will be managed by the Big Sandy RECC IT Department. All requests for amendments/additions must be approved by the Big Sandy RECC IT Department and President/General Manager

The manual will be subject to version control and when sufficient changes have been received, a full reissue will occur. All amendments will be circulated to the appropriate staff and will ensure that copies held within Big Sandy RECC are updated and the amendment record noted.

EXHIBIT 3
PAGE 6 OF 21

STANDARDS

EXHIBIT 3
PAGE 7 OF 21

RISK MANAGEMENT

Use of Computing Resources

- Computer resources may only be used by authorized individuals and authorized purposes.
- The playing of games and use of other forms of personal entertainment (gambling, etc.) on company resources is not allowed.
- Reasonable personal use of computer systems is allowed (e.g.: email, internet browsing). Social Media is currently allowed for CO-OP use and not personal.

Software Installation

- All software licenses will be maintained by the Big Sandy RECC IT Department.
- The introduction of software into Big Sandy RECC computer systems by persons other than the IT Dept. is not allowed.
- The IT Dept. will use the Big Sandy RECC Software Acquisition and Removal Standards as the foundation of software management.
- Only licensed copies (if not open source) of software can be installed. Open source software will need to be evaluated by the IT Dept. prior to install.
- Anyone suspecting unauthorized software present within a system must immediately inform the Big Sandy RECC IT Department. Upon notification:
    - The incident will be logged.
    - Appropriate follow-up action will be carried out to remove the software.

Copyright and Software Piracy

- Regular reviews are carried out to ensure the terms of software licenses are being complied with.
- Any unauthorized software will be isolated and access disabled.
- The copying of software other than for legitimate backup purposes is not allowed.

Remote Computing

- Remote computing devices must be registered with the Big

EXHIBIT 3
PAGE 8 OF 21

Sandy RECC IT Department.

- Remote connectivity into the network will be available via VPN or SSL-VPN only.
- Non Big Sandy RECC computing devices will have limited remote access.
- Secure ID will be utilized to gain access to the Big Sandy RECC LAN remotely.
- All Big Sandy RECC devices, including laptops, connecting to the company infrastructure must have anti-threat measures installed and in place:
    - Anti-virus software is installed and enabled.
    - Personal firewall is installed and enabled.
- Information classified as Big Sandy RECC Internal Use cannot be stored on any remote computing device that does not have user ID and password controlled access measures installed.

Internet Access

Big Sandy RECC, through the Internet, provides computing resources to its staff to access information, communicate, and retrieve and disseminate organization and business related information.

Use of the public Internet by Big Sandy RECC employees is permitted and encouraged where such use is suitable for business purposes in a manner that is consistent with the Big Sandy RECC Communications Policy and as part of the normal execution of an employee's job responsibilities. Example (Cell Service on personal devices)

Security:

- All connections must be made via a firewall protected, managed gateway.
- Never download files from unknown or suspicious sources.

Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so and appropriate protections are in place.

Unacceptable Use:

- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

EXHIBIT 3
PAGE 9 OF 21

- The following widely-used Internet programs represent significant potential security risks and are not allowed on any Big Sandy RECC computer. Many of these programs are packaged for download with spyware or dangerous malware which may seriously compromise your computers' Security.
    - Peer-to-peer(P2P) file sharing services such as Gnutella, Kazaa, Bit torrent, eDonkey
    - Video games, particularly any that might be downloaded from the Internet
    - Shareware utilities such as so called "Internet Accelerators"
    - Internet based Internet Relay Chat (IRC)
- Internet based Instant Messaging (IM) is considered an acceptable method of communication when configured accordingly:
    - Spark is the only authorized IM client. The following IM services are supported in the Spark client, all other services are blocked:
        - □ Windows Live service
        - □ Yahoo! Messenger service
        - □ Google Talk service

NOTE: Technical Services Administration maintains records giving details of the types of connections and users of that connection. All activity is logged and will record the source and destination of any traffic across the Internet gateway, together with details of the date, time, and protocol.

Email

Big Sandy RECC maintains electronic communication systems (email, voice mail, video conference, etc.) to assist in company business both internally and externally. These systems, including the equipment and the data stored in the system, are and remain the property of Big Sandy RECC.

Employees should be aware that even when messages are deleted or erased, it may still be possible to recreate the message; therefore, the ultimate privacy of message control may not be assured.

EXHIBIT 3
PAGE 10 OF 21

While electronic communication systems may accommodate the use of passwords for security, this control does not ensure message confidentiality.

Security:

- DO NOT send confidential information when using email or any other messaging method that could be intercepted.
    - Credit Card number, PIN/PAN
    - Bank information: account number, routing information
    - Social Security numbers
    - Username & password combination
- When using email, don't open attachments unless you are expecting them. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.
- If you receive an email from an unknown user with attachments, that user should be blocked. This can be achieved within the settings of your email software program.
- Check any embedded links within emails to verify they point to the expected location before clicking the link. Generally, hovering your mouse cursor above the link will display a "popup" indicating the target location – if the displayed link and the popup link differ, the intent might be malicious.
- Designated anti-virus software must remain installed and active at all times. Do not disable or remove the anti-virus software.

Unacceptable Use:

- Employees and other authorized users must not use offensive or obscene, derogatory or slanderous remarks in any electronic mail messages.
- Employees must not participate in, encourage, or forward any email advertising non-company goods or services.
- The propagation of chain e-mail[8] messages are not allowed.

Monitoring:

- Big Sandy RECC is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is

EXHIBIT 3
PAGE 11 OF 21

occasionally necessary, as authorized by management, to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

- Big Sandy RECC reserves the right to retrieve and review any messages composed, sent or received.

ACCESS CONTROL

Controlling Access Rights

- Formal documented procedures must be followed for requesting, authorizing, granting, and enabling access to computer resources. An asset tracking form will be used to issue and maintain computer resources.
- The use of system utilities and devices capable of bypassing system access controls must be strictly limited and monitored. The Big Sandy RECC IT Department will maintain a log of the usage of such tools.

User Identification

- All Big Sandy RECC domain user IDs must be allocated by the Big Sandy RECC IT Division.
- Unauthorized use of user IDs is considered to be a breach of the Big Sandy RECC Employee Conduct.
- For auditing purposes, generic or "ownerless" user IDs are not recommended, each user ID should be assigned to one individual only.

Password

- Passwords must:
    - Not be displayed by the system on entry
    - Not be written down
    - Not be recorded in audit
    - Not be the same as the user ID
    - Not be manufacturer supplied
- Big Sandy RECC domain group policy "password standards" will enforce the following:

- Be a minimum of 8 characters long
- Contain characters from three of the following four categories:
  - English uppercase (ex: A-Z)
  - English lowercase (ex: a-z)
  - Base 10 digits (ex: 0-9)
  - Non alpha characters (ex: !, $, #, %, etc.)
- Be changed at least every 180 days (this only applies to computers) Exempt (UPN, Online utility, Exceleron, TNS, CRC,Milsoft and emails)

Remote System Access

- Remote system access can only be obtained via VPN/ SSL VPN connectivity and a secure ID that was provided to you.
- All hosts that are connected to Big Sandy RECC internal networks via remote access technologies must use the most up-to-date anti-virus software

PHYSICAL AND ENVIRONMENTAL SECURITY CONTROLS

Server Rooms

- All visitors must be accompanied by authorized personnel while in controlled areas.
- All third party contractors, visitors, etc. must not be left alone in the computer rooms or other sensitive locations.
  - Details of third party contractors' portable devices/media (USB memory, CDs, etc.) On-site usage needs to be documented.
- Server rooms will be secured and access controlled.

Network Security

- Access to network equipment is restricted to authorized personnel only.
- Only authorized personnel are allowed to connect management- approved devices to the network. Such devices include workstations and servers owned by Big Sandy RECC that comply with the configuration standards of Big Sandy RECC, routers, switches, firewalls, managed wireless access points and network management/monitoring devices. Devices that are not management-approved include modems and unmanaged wireless access points. Installation and maintenance of these devices are restricted to the Big Sandy RECC IT Dept.
- Network configuration information is maintained and the network logs compared to this to identify unrecognized devices.

EXHIBIT 3
PAGE 13 OF 21

- When a third party contractor's device (i.e. laptop) is to be connected to the network, it must be authorized by the Big Sandy RECC IT department to ensure it is properly patched and anti-virus software is running.
- Users are not allowed to attach devices or PCs running host port scanning, "sniffers", or network filtering software.

Employee Identification

At the present time, Big Sandy RECC does not require its employees to wear a photo ID bade; however every employee is issued a keyless entry device. There should be no sharing of the keyless entry devices and it must be reported to the IT dept. immediately if one becomes lost.

DATA SECURITY

Information Classification

Information needs to be protected from unauthorized access, modification, disclosure and destruction. Classification of information into categories is necessary to help identify a framework for evaluating the information's relative value and the appropriate controls required to preserve its value to Big Sandy RECC.

- Two basic classifications of information have been established:
  - Public: Information that has been made available for public distribution through authorized company channels. Examples:
    - □ Corporate annual report
    - □ Public service bulletins, marketing brochures, social media and advertisements
  - Big Sandy RECC Internal Use: Information that is intended for use by employees when conducting company business. Most information used in Big Sandy RECC would be classified Big Sandy RECC Internal Use. Guidelines for handling such information can be found in the Big Sandy RECC Sensitive Data Protection Guidelines document.
    Examples:
    - □ Operational business information and reports and non- company information that is subject to nondisclosure agreement
    - □ Company policy, standards and procedures unless stated otherwise
    - □ Personnel records, Big Sandy RECC Member/Customer data or Big Sandy RECC Member/Customer consumer personal identifying information, and health insurance records.

EXHIBIT 3
PAGE 14 OF 21

Sensitive Information Use & Handling

- Sensitive information for which access has been authorized may only be used for the Purposes identified to and authorized by the information owner.
- All sensitive data (Big Sandy RECC or Big Sandy RECC Member/Customer employee personal identifying information or Big Sandy RECC Member/ Customer consumer personal identifying information[9]) must be sanitized – sensitive data removed – prior to usage in:
    - Testing/debugging environments.
    - Demo environments.
    - Contact Adam Ferguson at extension 214 in the Big Sandy RECC IT Dept. to establish and maintain proper data sanitization procedures.

Email

- Users must not originate or forward Big Sandy RECC Internal Use information from/to a personal account (yahoo, hotmail, gmail, etc.)
- Users must not forward or further distribute company confidential information, inside or outside Big Sandy RECC, without the authorization of the originator or appropriate management.
- Any electronic messages intended for an outside entity that contains Big Sandy RECC Internal Use information must be encrypted. (See Big Sandy RECC Technical Services or Big Sandy RECC Security Department)
- Double check the recipient to avoid inadvertent information leakage.

Portable Devices

- Sensitive Big Sandy RECC data must not be transmitted via wireless to or from a portable computing device unless approved wireless encryption techniques[4] are utilized.
- Sensitive Big Sandy RECC data must not be accessed and/or transmitted via public computer/terminal unless approved encryption techniques[4] are utilized.
- Big Sandy RECC must ensure that all company data and software are recovered, deleted, and securely overwritten as appropriate from company owned portable computing devices when the user's employment or contract terminates, or when the portable computing device is no longer authorized for work use. Please contact the Helpdesk to have the portable device sanitized.

EXHIBIT 3
PAGE 15 OF 21

Sensitive Information Use & Handling

- Sensitive information for which access has been authorized may only be used for the Purposes identified to and authorized by the information owner.
- All sensitive data (Big Sandy RECC or Big Sandy RECC Member/Customer employee personal identifying information or Big Sandy RECC Member/ Customer consumer personal identifying information[9]) must be sanitized – sensitive data removed – prior to usage in:
    - Testing/debugging environments.
    - Demo environments.
    - Contact Adam Ferguson at extension 214 in the Big Sandy RECC IT Dept. to establish and maintain proper data sanitization procedures.

Email

- Users must not originate or forward Big Sandy RECC Internal Use information from/to a personal account (yahoo, hotmail, gmail, etc.)
- Users must not forward or further distribute company confidential information, inside or outside Big Sandy RECC, without the authorization of the originator or appropriate management.
- Any electronic messages intended for an outside entity that contains Big Sandy RECC Internal Use information must be encrypted. (See Big Sandy RECC Technical Services or Big Sandy RECC Security Department)
- Double check the recipient to avoid inadvertent information leakage.

Portable Devices

- Sensitive Big Sandy RECC data must not be transmitted via wireless to or from a portable computing device unless approved wireless encryption techniques[4] are utilized.
- Big Sandy RECC must ensure that all company data and software are recovered, deleted, and securely overwritten as appropriate from company owned portable computing devices when the user's employment or contract terminates, or when the portable computing device is no longer authorized for work use. Please contact the Helpdesk to have the portable device sanitized.
- A personal firewall must be installed and active when connecting your portable device to non-Big Sandy RECC networks, especially wireless networks.

EXHIBIT 3
PAGE 16 OF 21

PROCEDURES & GUIDELINES

EXHIBIT 3
PAGE 17 OF 21

Big Sandy RECC PORTABLE DEVICE SECURITY PROCEDURES

Physical Security

- To report a missing portable device, call Adam Ferguson[3] in the Big Sandy RECC IT Dept.
- Users must protect Big Sandy RECC–owned (or authorized) portable computing devices and portable media[2] from unauthorized access. Physical security measures shall, at a minimum, include the following:
    - Devices must not be left unattended without employing adequate safeguards such as cable locks, restricted access environments, or by simply taking it with you. Portable computing devices and portable media must be stored in a secure environment.
    - Portable computing devices and portable media must remain under visual control while traveling. If visual control cannot be maintained, then necessary safeguards shall be employed to protect the physical device and portable media.
    - Tape an identification tag, such as an asset tag or business card, to the top of your laptop. This makes your laptop easy to recognize when you send it through airport X-ray, and makes it easier to return to you if it gets lost.
- Safeguards shall be taken to avoid unauthorized viewing of sensitive or confidential data in public or common areas.
- While locking your PC to a desk with a cable lock may keep someone from walking away with your laptop, there is little you can do to keep someone from stealing a PCMCIA card or USB storage device that is sticking out of the side of your machine. When not in use, eject these cards from the laptop bay and lock them in a safe place.
- When you travel or commute, the following guidelines can help guard against portable device and portable media thieves:
    - Never leave your laptop, laptop bag, portable

EXHIBIT 3
PAGE 18 OF 21

device or portable media unattended.

- If possible, carry your laptop in an inconspicuous bag (ex: backpack)
- Keep your arm (or leg, if you set the bag down) through the strap.
- Never leave your laptop, laptop bag or portable device or portable media in a visible area of a car. It is best to take it with you out of the car whenever possible.
- If you place your laptop in the trunk of your car, place it there before you leave for your destination, not after you are parked at your destination. Thieves watch for people who place items in the trunk and then walk away from their car.
- Use a hotel safe to store your laptop when you are out of the room for longer periods. If a safe is not available, place the portable device out of sight – such as under the bed or in a closet.
- Take extra care at times and places where you can be easily distracted, such as:
  - □ At an airline or rental car counter
  - □ While going through airport X-ray
  - □ While speaking to someone, whether in person or on the phone
  - □ While on an airplane, bus or train
  - □ While loading luggage into a taxi – keep your laptop bag with you inside the taxi
  - □ When a stranger distracts you by asking for assistance or bumping into you – it could be a decoy

Data Security

Given their small size and portable nature, it is more likely that these portable computing devices will fall into the wrong hands than a desktop system. The following guidelines are used to govern the management and maintenance of personal and company data on portable computing devices:

- Sensitive Big Sandy RECC data should not be stored on portable computing devices. However, in the event that there is no alternative to local storage, all sensitive Big Sandy RECC data stored on portable computing devices must be secured in accordance with Big Sandy RECC's encryption procedures. Methods for securing information maintained on portable computing devices include, but are not limited to:

EXHIBIT 3
PAGE 19 OF 21

  - Personal Firewalls[6]
  - Screen Locking[7]
  - Data/Application encryption
  - Security Tokens
- Consider backing up your laptop or portable device before you do any extended traveling that may put your data at risk.
- Infrared ports should be disabled. If it is not, or are unsure how to check the status, please contact the Helpdesk to disable it.
- When the wireless adapter in your portable device is not being used, it is recommended that you disable it.
  - Dell laptops (D6x model): Function (Fn) & F2 keys.
  - Smartphones: will vary depending on the vendor.
  - If you are unsure how to check the status or disable the adapter, please contact the Helpdesk.

Blogs, Social Networks, Wikis Usage Guidelines

Web 2.0 refers to a perceived second generation of Web-based services—such as social networking sites (ex: Facebook.com, Twitter.com), wikis and other communication methodologies—that emphasize online collaboration and sharing among users.

Big Sandy RECC believes in the importance of open exchange and learning -- between Big Sandy RECC and its Members/Customers, and among the many constituents of our business. The rapidly growing usage of blogs and online dialogue are important arenas for that kind of engagement and learning, but can expose the company network to additional threats.

The following are general best practices when using these services:

- Most blogs publish RSS feeds that others can subscribe to, so remember that others, including your colleagues, may be actively reading what you write.
- Remember that you are responsible for your commentary and that bloggers can be held personally liable for any commentary deemed defamatory, obscene, proprietary, or libelous. Think of what you post in the same way as statements you might make to the media, or emails you might

EXHIBIT 3
PAGE 20 OF 21

send to people you don't know. If you wouldn't include it in those, don't post it.

- Never disclose any information – including textual or visual material – that is confidential or proprietary to Big Sandy RECC, or any third party that has disclosed information to us (e.g. members).
  Example:
  - Company direction, customer relations data.
  - Firewall/network/server configurations, log data.
- You should make it clear that the views you express are yours alone. You may want to use the following form of words on your weblog, weblog posting, or website: The views expressed on this [blog; website] are my own and do not necessarily reflect the views of my employer

IT Asset Control & Disposal Policy

Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable organizational assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

Purpose

This policy is designed to protect the organizational resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

EXHIBIT 3
PAGE 21 OF 21

IT Asset Types

This section categorized the types of assets subject to tracking.

- Desktop workstations
- Laptop mobile computers
- Printers, Copiers, FAX machines, multifunction machines
- Handheld devices
- Scanners
- Servers
- Firewalls
- Routers
- Switches
- Memory devices

Asset Disposal Guidelines:

Asset disposal is a special case since the asset must have any sensitive data removed during or prior to disposal. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. None (Unclassified) - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
2. Low (Sensitive) - Erase the data using any means such as reformatting or degaussing.
3. Medium (Confidential) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. High (Secret) - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to specified in a Media Data Removal Procedure document by asset type including:
    1. Floppy disk
    2. Memory stick
    3. CD ROM disk
    4. Storage tape
    5. Hard drive.
    6. RAM memory
    7. ROM memory or ROM memory devices.
5. If the asset is to be scraped completely, removal of the hard drives and making the disk unreadable (such as smashing the drives) is recommended.